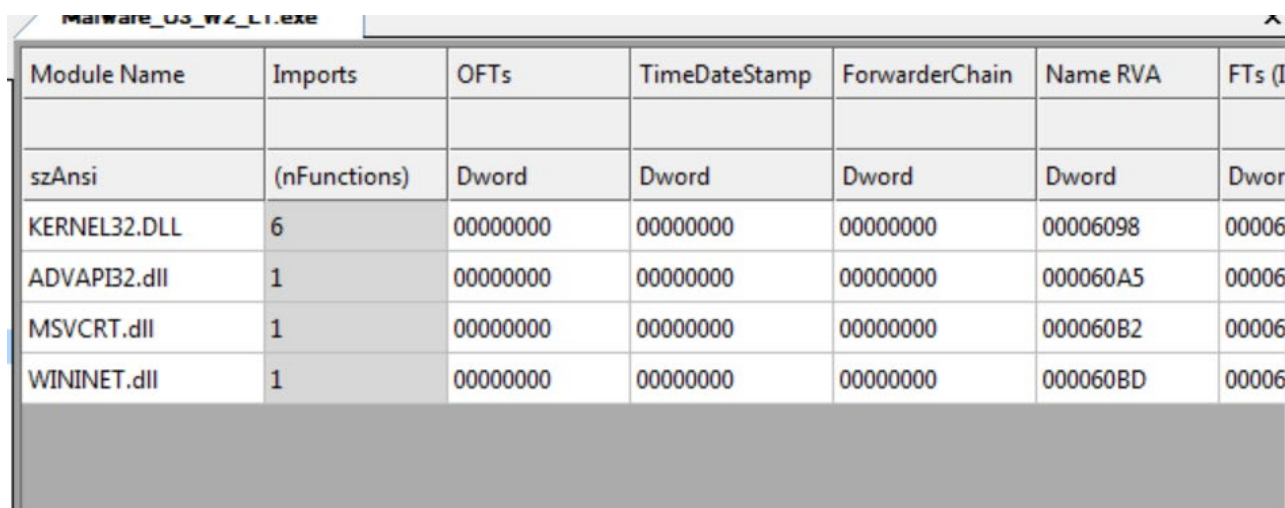


S10 - L1 MALWARE ANALISYS

L'immagine di seguito mostra una schermata del software **CFF Explorer**, utilizzato per analizzare i file eseguibili di Windows.



Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (I
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dwor
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006
WININET.dll	1	00000000	00000000	00000000	000060BD	00006

L'immagine mostra la tabella delle importazioni del file eseguibile, evidenziando le librerie DLL (Dynamic Link Library) che il malware carica e utilizza. Ecco una spiegazione delle librerie elencate:

1. **KERNEL32.DLL:**

- Questa è una delle librerie fondamentali di Windows e contiene funzioni per la gestione della memoria, dei file, dei processi e dei thread, oltre a molte altre funzioni di sistema di basso livello. Il fatto che il malware importi funzioni da questa libreria suggerisce che potrebbe voler manipolare file, gestire processi o eseguire altre operazioni di sistema.

2. **ADVAPI32.dll:**

- La libreria ADVAPI32 contiene funzioni avanzate API di Windows, molte delle quali sono legate alla gestione della sicurezza e delle operazioni del registro. Importare funzioni da questa libreria può indicare che il malware cerca di accedere o modificare voci del registro di sistema o gestire i privilegi e le autorizzazioni degli utenti.

3. **MSVCRT.dll:**

- Questa libreria è parte del Microsoft Visual C++ Runtime e contiene funzioni di base per la gestione di input/output, stringhe, gestione della memoria e altre

operazioni standard in C. Il malware potrebbe usare funzioni da questa libreria per operazioni di calcolo e gestione dei dati.

4. WININET.dll:

- WININET è una libreria di Windows che offre funzioni per l'accesso a Internet, inclusi protocolli come HTTP e FTP. L'importazione di questa libreria è spesso un indicatore che il malware potrebbe tentare di comunicare con server remoti, scaricare o caricare dati, o svolgere altre attività di rete.

Considerazioni sulle librerie

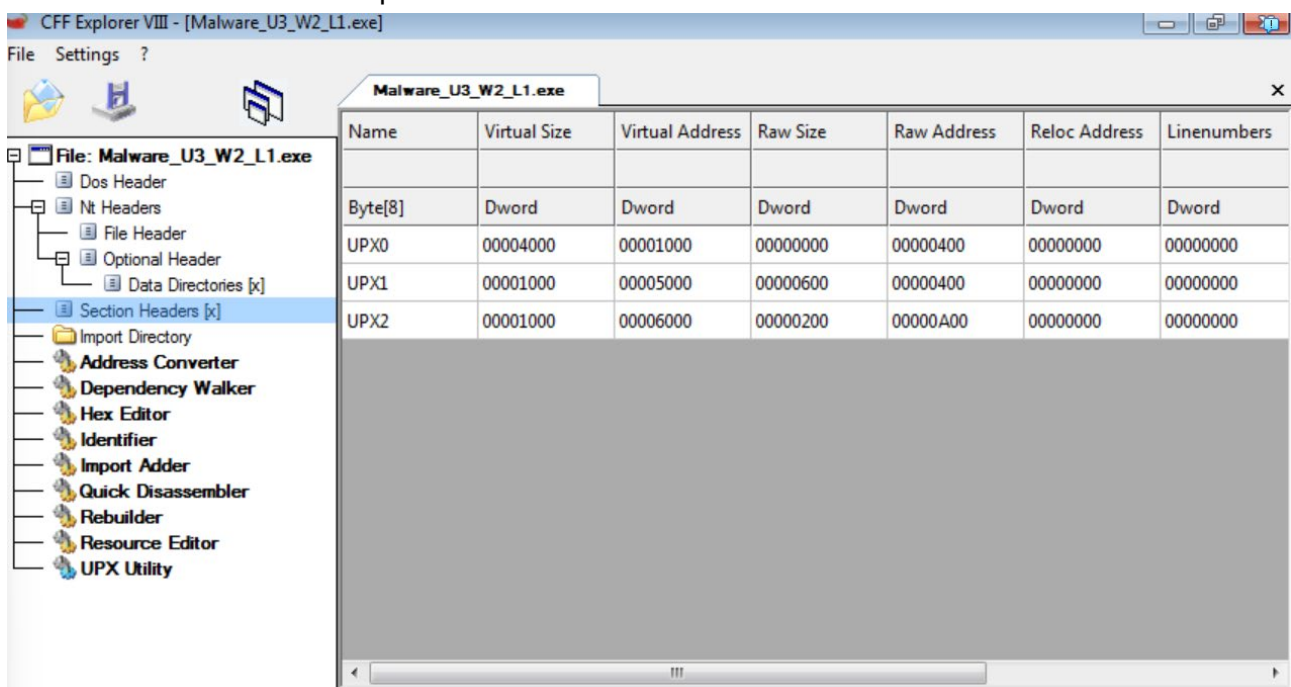
L'uso di queste librerie suggerisce che il malware potrebbe essere progettato per eseguire una serie di operazioni, tra cui:

- **Manipolazione di file e processi** (KERNEL32.DLL)
- **Modifiche al registro di sistema o gestione delle autorizzazioni** (ADVAPI32.dll)
- **Comunicazioni di rete** (WININET.dll)
- **Operazioni generali di calcolo e gestione dei dati** (MSVCRT.dll)

In questa immagine invece abbiamo la sezione "**Section Headers**", che contiene informazioni sulle varie sezioni di un eseguibile. Le sezioni indicate sono "**UPX0**", "**UPX1**" e "**UPX2**".

Le sezioni indicate sono etichettate con il prefisso "**UPX**", che suggerisce che il file è stato compresso utilizzando **UPX (Ultimate Packer for eXecutables)**.

UPX è un compressore di eseguibili che riduce le dimensioni del file, rendendolo più difficile da analizzare senza decomprimerlo.



Di seguito invece potete trovare una spiegazione un po' più dettagliata delle varie sezioni che compongono il malware:

- **UPX0:** Tipicamente contiene il codice compresso del programma.
- **UPX1:** Di solito è la sezione che contiene l'originale (non compresso) del programma.
- **UPX2:** Può essere utilizzata per dati o codice aggiuntivi.
- **Virtual Size:** Indica la dimensione della sezione in memoria quando il file viene caricato. Spesso è più grande della dimensione fisica su disco a causa di allineamenti o dati non compressi.
- **Virtual Address:** Questo è l'indirizzo in memoria in cui la sezione sarà caricata.
- **Raw Size:** La dimensione della sezione nel file su disco.
- **Raw Address:** Indica dove inizia la sezione all'interno del file su disco.
- **Reloc Address e Linenumbers:** Questi campi non contengono informazioni significative in questo contesto, spesso sono zero per file compressi o protetti.

Per un'analisi completa e per esaminare il comportamento potenziale del malware, sarebbe necessario decomprimere il file e analizzare ulteriormente il codice e le risorse contenute in queste sezioni.